KVATERNIONOVÉ ALGEBRY S PROGRAMEM SAGE

LENKA MACÁLKOVÁ

Abstrakt. V tomto článku si klademe za cíl seznámit čtenáře s využitím systému SAGE v souvislosti s výpočty na kvaternionových algebrách. První část je zaměřena na práci s prvky kvaternionové algebry, ve druhé části se věnujeme ideálům a řádům kvaternionových algeber.

Úvod

V první části článku se seznámíme se systémem počítačové algebry SAGE. Poté se budeme věnovat příkladům, ve kterých použijeme SAGE v souvislosti s kvaternionovými algebrami. Ve druhé části pak uvedeme definice ideálu a řádu kvaternionové algebry. Dále se zabýváme pojmem diskriminantu a maximálního řádu kvaternionové algebry.

1. Seznámení se systémem SAGE

SAGE je open-source systém počítačové algebry, který je vytvořený v programovacím jazyce Python. Je k dispozici pro všechny platformy a je možné jej stáhnout na `http://www.sagemath.org/`, nebo lze využít online rozhraní (přístupné na stejné adrese).

Nyní se lehce seznámíme s ovládáním. Řádek s příkazem bude vždy začínat „sage:“

```
sage: 3−2+5∗3−7/3
    41/3
sage: cos(pi/2)
    0
```

Z příkladu je vidět, že základní matematické operace a funkce není složité zapsat. My se v tomto článku zaměříme na použití SAGE v souvislosti s kvaternionovými algebrami.

Začneme tím, že si připomeneme definici kvaternionové algebry. V celém textu budeme pracovat s tělesem, jehož charakteristika není dva.

2010 *MSC.* Primární 11R52, 11-04.

Klíčová slova. Kvaternionová algebra, SAGE, ideál, řád.

Práce byla podporována projektem A-Math-Net – Síť pro transfer znalostí v aplikované matematice (CZ.1.07/2.4.00/17.0100).

Definice 1.1. *Kvaternionovou algebrou* A nad tělesem F rozumíme vektorový prostor dimenze čtyři s bázovými vektory $1, i, j, k$, kde neutrálním prvkem vzhledem k operaci násobení na A je 1 a dále platí, že

$$i^2 = a, \quad j^2 = b, \quad ij = -ji = k,$$

kde $a, b \in F^*$.

Poznámka 1.2. Pro těleso F s charakteristikou dva je definice kvaternionové algebry shodná až na zavedení operace násobení. Ta je v tomto případě definována následovně:

$$i^2 + i = a, \quad j^2 = b, \quad ij = j(1 + i) = k,$$

kde $a \in F, b \in F^*$.

Nyní se podíváme, jakým způsobem zadat kvaternionovou algebru v SAGE. Pod příkazem

```
sage: A.<i,j,k>=QuaternionAlgebra(QQ,−1,2)
```

rozumíme: Sestroj kvaternionovou algebru A s bází $1, i, j, k$, nad tělesem racionálních čísel (tj. QQ), kde $a = -1, b = 2$. Pokud bychom chtěli kvaternionovou algebru nad tělesem K o dvaceti pěti prvcích, kde $a = -1, b = 3$, zadáme

```
sage: B.<i,j,k>=QuaternionAlgebra(GF(25,'z'),−1,3)
```

Symbolem `z` v příkazu `GF(25,'z')` označujeme kořen ireducibilního polynomu, podle nějž provádíme operaci modulo v tělese $GF(25)$.

Uvědomme si, že některé kvaternionové algebry jsou okruhy s dělením (tj. každý nenulový prvek má inverzi), jiné nikoli. Nejznámějším příkladem kvaternionové algebry s dělením jsou Hamiltonovy kvaterniony, což je kvaternionová algebra nad reálnými čísly, kde $a = b = -1$. Kvaternionovou algebrou, která není okruhem s dělením (tzn. má dělitele nuly), je například kvaternionová algebra nad reálnými čísly, kde $a = 1$, $b = -1$. Zde je dělitelem nuly prvek $1 + i$, neboť $(1 + i)(1 - i) = 0$. Pokud bychom chtěli vědět, zda je daná kvaternionová algebra nad nekonečným tělesem okruhem s dělením, můžeme použít funkci `is_division_algebra()`. SAGE vrátí `True` v kladném případě, v opačném vrátí `False`:

```
sage: B.<i,j,k>=QuaternionAlgebra(GF(25, 'z'), −1,3)
sage: B.is_division_algebra()
   False
sage: A.<i,j,k>=QuaternionAlgebra(QQ, −1,3)
sage: A.is_division_algebra()
   True
```

Podobnou booleovskou funkcí je například funkce `is_finite()` nebo funkce `is_integral_domain()`. Z jejich názvu si čtenář jistě snadno pochopí, k čemu tyto funkce slouží. Nabízí se otázka, jak probíhají operace s prvky z kvaternionových algeber. Pro příklad můžeme najít dva náhodné prvky x, y z algebry A a spočítat jejich součin a součet:

```
sage: A.<i,j,k>=QuaternionAlgebra(QQ, −1,3)
sage: x=A.random_element()
sage: x
  −1 + 4∗ii + jj + 1/3∗kk
sage: y=A.random_element()
sage: y
  15/2 + 1/18∗ii − 2∗jj
sage: x+y
  13/2 + 73/18∗ii − jj + 1/3∗kk
sage: x∗y
  41/18 + 599/18∗ii + 257/27∗jj − 50/9∗kk
```

Pro kvaterninovou algebru A a každý její prvek $x = a_0 + a_1 i + a_2 j + a_3 k$ definujeme stopu $\mathrm{Tr}(x)$ a normu $\mathrm{N}(x)$ jako

$$\mathrm{Tr}(x) = 2a_0, \quad \mathrm{N}(x) = a_0^2 - a_1^2 a - a_2^2 b + a_3^2 ab.$$

Funkce `reduced_norm()` a `reduced_trace()` slouží pro výpočet normy a stopy prvku. Spočítejme tedy pro ukázku normu a stopu prvku x uvedeného výše:

```
sage: x.reduced_norm()
  203/9
sage: x.reduced_trace()
  −2
```

2. Řády kvaternionových algeber

Před tím, než uvedeme další příklady použití programu SAGE, zavedeme pojem řádu kvaternionové algebry. V této části budeme uvažovat Dedekindův okruh R a jeho podílové těleso K.

Definice 2.1. Mějme vektorový prostor V nad tělesem K. *R-mřížkou* nad V rozumíme konečně generovaný R-modul obsažený ve V. Mřížka L je *úplná*, jestliže $K \otimes_R L \simeq V$.

Definice 2.2. Nechť A je kvaternionová algebra nad K. Libovolnou úplnou R-mřížku nazveme *ideálem*. Je-li taková mřížka navíc okruhem, tak ji nazýváme *řádem*.

Definice 2.3. Nechť I je ideál kvaternionové algebry A, pak *levým řádem* ideálu I nazýváme množinu

$$\mathcal{O}_l(I) = \{a \in A | aI \subset I\}.$$

Pravý řád ideálu I analogicky definujeme jako

$$\mathcal{O}_r(I) = \{a \in A | Ia \subset I\}.$$

Pro práci s ideály a řády kvaternionových algeber slouží v SAGE některé funkce. Tyto funkce můžeme použít pouze pro kvaternionové algebry nad racionálními čísly. Začneme s funkcí `ideal()`, která vrací ideál s danými generátory nad $\mathbb{Z}$.

Funkce `basis()`, která je použita v následujícím příkladu, vrací bázi. V následujícím příkladu zadáme ideál I pomocí báze a to tak, že každý prvek báze I je trojnásobkem prvku báze A.

```
sage: A=QuaternionAlgebra(QQ,−1,−13)
sage: I=A.ideal([3∗a for a in A.basis()])
sage:I
  Fractional ideal (3, 3∗i,3∗j, 3∗k)
```

Pokud bychom chtěli zjistit, zda je daná množina ideálem, stačí při zadávání ideálu přidat argument `check=False`, např.

```
A.ideal([4∗a for a in A.basis()], check=False)}
```

Řád kvaternionové algebry můžeme zadat stejným způsobem jako ideál, jen místo funkce `ideal()` využijeme funkce `quaternion_order()`. Pokud budeme chtít zkontrolovat, zda se jedná o řád, můžeme opět použít `check=False`. SAGE nabízí i funkce `left_order()` a `right_order()` pro práci s levými a pravými řády pro daný ideál I. Pro ukázku spočteme levý řád ideálu z předchozího případu.

```
sage: A=QuaternionAlgebra(QQ,−1,−13)
sage: Q=A.quaternion_order([1,2∗i,2∗j,2∗k]) sage: Q
  Order of Quaternion Algebra (−1, −13) with base ring Rational
     Field with basis (1, 2∗i, 2∗j, 2∗k)
sage: I.left_order()
  Order of Quaternion Algebra (−1, −13) with base ring Rational
     Field with basis (1, i, j, k)
```

V souvislosti s řády kvaternionových algeber je třeba zmínit také maximální řády.

Definice 2.4. *Maximálním řádem* $\mathcal{O}$ kvaternionové algebry A, rozumíme takový řád, že neexistuje žádný řád $\mathcal{O}'$ s vlastností $\mathcal{O} \subset \mathcal{O}' \subset A$.

Věta 2.5. *Každý řád kvaternionové algebry je podřádem nějakého maximálního řádu.*

Bohužel v současné době nemáme algoritmus, podle kterého bychom byli schopni rychle určit maximální řády kvaternionových algeber. SAGE je schopen vypočítat maximální řád pouze v případě, kdy se jedná o kvaternionovou algebru nad $\mathbb{Q}$, která má prvočíselný diskriminant. Tomuto pojmu se budeme nyní krátce věnovat.

Nejprve seznámíme čtenáře s pojmem p-adické metriky a p-adických čísel.

Definice 2.6. Mějme $n \in Z$ a p je prvočíslo. Symbolem $v_p(n)$ budeme označovat největší $a \in \mathbb{Z}$, pro které platí $p^a | n$. Pro racionální číslo v základním tvaru $\frac{m}{n}$ položme $v_p(\frac{m}{n}) = v_p(m) - v_p(n)$.

Definice 2.7. Mějme prvočíslo p. Pro libovolné $r \in \mathbb{Q}$ v základním tvaru definujme *p-adickou normu* $|r|_p$ tak, že $|r|_p = p^{-v_p(r)}$ pro $r \neq 0$ a $|r|_p = 0$ pro $r = 0$.

S pomocí p-adické normy lze na racionálních číslech zavést tzv. *p-adickou metriku* ϱ_p tak, že pro každá dvě racionální čísla x, y je jejich vzdálenost v p-adické metrice $\varrho_p(x, y) = |x - y|_p$. Pokud provedeme zúplnění racionálních čísel vzhledem k této metrice, dostáváme tzv. *p-adická čísla* $\mathbb{Q}_p$, tedy v závislosti na volbě prvočísla 2-adická, 3-adická, ... Lze dokázat, že p-adická čísla tvoří těleso. V případě zájmu si dovolujeme čtenáře odkázat na [2].

Definice 2.8. Mějme $a, b \in K$. Hilbertovým symbolem vzhledem k tělesu K rozumíme

$$(a, b) = \begin{cases} 1, & \text{rovnice } ax^2 + by^2 = z^2 \text{ má nenulové řešení v } K \\ -1, & \text{jinak} \end{cases}$$

Hilbertův symbol v tělese $\mathbb{Q}_p$ budeme značit $(a, b)_p$.

Definice 2.9. Mějme kvaternionovou algebru A nad Q, kde $i^2 = a$, $j^2 = b$. Označme X množinu všech prvočísel, kdy $(a, b)_p = -1$. Pak *diskriminantem* d kvaternionové algebry, rozumíme výraz

$$d = \prod_{p \in X} p.$$

Nyní se vrátíme k výpočtům v systému SAGE. Pro výpočet Hilbertova symbolu $(a, b)_p$ lze použít funkci `hilbert_symbol()` s parametry `a,b,p`. Pokud bychom chtěli zjistit všechna prvočísla, která se ve výpočtu diskriminantu vyskytují, využijeme funkce `ramified_primes()`. Pro samotný výpočet diskriminantu pak slouží funkce `discriminant()`.

```
sage: A=QuaternionAlgebra(QQ,−5,−13)
sage: hilbert_symbol(−5,−13,2)
  −1
sage: hilbert_symbol(−5,−13,11)
   1
sage: A.ramified_primes()
  [2,5,13]
sage: A.discriminant()
  130
```

Nyní se vrátíme zpět k maximálnímu řádu. Jak už bylo řečeno, SAGE vypočítá maximální řád pouze pro kvaterninovou algebru nad $\mathbb{Q}$ s prvočíselným diskriminantem. V první případě ukážeme výpočet na Hamiltonových kvaternionech. Jejím maximálním řádem jsou tzv. Hurwitzovy kvaterniony.

```
sage: A.<i,j,k>=QuaternionAlgebra(QQ,−1,−1)
sage: A.discriminant()
  2
sage: A.maximal_order()
  Order of Quaternion Algebra (−1, −1) with base ring Rational
     Field with basis (1/2 + 1/2∗i + 1/2∗j + 1/2∗k, i, j, k)
sage: B.<i,j,k>=QuaternionAlgebra(QQ,−7,−11) sage: B.discriminant()
  7
B.maximal_order()
  Order of Quaternion Algebra (−7, −11) with base ring Rational
     Field with basis (1/2 + 1/2∗j, 1/2∗i + 1/2∗k, j, k)
```

SAGE obsahuje ještě mnoho dalších funkcí, které lze použít při zkoumání vlastností kvaternionových algeber, jsou však vysoce nad rámec tohoto textu. Čtenáře proto odkážeme na referenční manuál, který najde na stránkách [3].

Reference

[1] C. Maclachlan, A. W. Reid: *The Arithmetic of Hyperbolic 3-Manifolds*, Springer-Verlag, New York, 2003.
[2] J. Preszler: *Introduction to p-adic numbers*, University of Utah, 2005.
[3] SAGE: *Sage's Reference Manual*, http://www.sagemath.org/doc/reference/.

Lenka Macálková, Ústav matematiky a statistiky, Přírodovědecká fakulta, Masarykova univerzita v Brně, Kotlářská 2, 611 37 Brno, Česká republika,
e-mail: macalkoval@gmail.com